



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/622,709	07/21/2003	Christopher Andrew Barton	03.025.01	2960
7590 Zilka-Kotab, PC P.O. Box 721120 San Jose, CA 95172-1120		01/12/2007	EXAMINER REVAK, CHRISTOPHER A	
			ART UNIT	PAPER NUMBER
			2131	
SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE		
3 MONTHS	01/12/2007	PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/622,709	BARTON ET AL.	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 21 July 2003.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-24 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-24 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on 7/21/03 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO/SB/08)
 Paper No(s)/Mail Date 11/5/03.

4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____.
 5) Notice of Informal Patent Application
 6) Other: _____.

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statement (IDS) submitted on November 5, 2003 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-24 are rejected under 35 U.S.C. 102(e) as being anticipated by Le Pennec et al, U.S. Patent 6,976,271.

As per claim 1, it is taught by Le Pennec et al of a computer program product carrying a computer program operable to control a computer to detect malware within a computer file, said computer program comprising identifying code operable to identify said computer file as potentially being a specific known malware free computer file; determining code operable to determine one or more attributes of said computer file; and comparing code operable to compare said one or more attributes determined from

Art Unit: 2131

said computer file with corresponding stored attributes of said specific known malware free computer file; wherein if said attributes match, then confirming said computer file as being said specific known malware free computer file; and if said attributes do not match then performing further malware detection processing upon said computer file (col. 9, line 10 through col. 10, line 27; col. 12, lines 43-64; col. 13, lines 49-57; col. 14, lines 44-59; and col. 15, lines 17-26).

As per claims 2,10, and 18, it is disclosed by Le Pennec et al wherein said identifying code is operable to compare one or more of file name, storage location and file size of said computer file with a corresponding one or more of file name, storage location and file size of said specific known malware free computer file (col. 16, lines 10-36).

As per claims 3,11, and 19, Le Pennec et al teaches wherein said computer file is identified as being potentially one specific known malware free computer file from among a plurality of specific known malware free computer files (col. 7, lines 42-47).

As per claims 4,12, and 20, Le Pennec et al discloses wherein said one or more attributes include one of more of a checksum calculated from at least a portion of said computer file; and content of at least a portion of said computer file (col. 11, lines 31-40).

As per claim 5,13, and 21, it is taught by Le Pennec et al wherein said further malware detection processing includes detecting within said computer file one or more characteristic corresponding to a known malware file (col. 4, lines 3-16).

As per claims 6,14, and 22, it is disclosed by Le Pennec et al wherein said one or more characteristic corresponding to a known malware file are stored within a malware signature file (col. 4, lines 3-16).

As per claims 7,15, and 23, Le Pennec et al teaches wherein said specific known malware free computer file is one of an operating system file (col. 7, lines 42-47).

As per claims 8,16, and 24, it is taught by Le Pennec et al wherein said malware being detected is one of a computer virus (col. 13, lines 49-57).

As per claim 9, it is disclosed by Le Pennec et al of a method of detecting malware within a computer file, said method comprising the steps of identifying said computer file as potentially being a specific known malware free computer file; determining one or more attributes of said computer file; and comparing said one or more attributes determined from said computer file with corresponding stored attributes of said specific known malware free computer file; wherein if said attributes match, then confirming said computer file as being said specific known malware free computer file; and if said attributes do not match then performing further malware detection processing upon said computer file (col. 9, line 10 through col. 10, line 27; col. 12, lines 43-64; col. 13, lines 49-57; col. 14, lines 44-59; and col. 15, lines 17-26).

As per claim 17, Le Pennec et al teaches of an apparatus for detecting malware within a computer file, said apparatus comprising identifying logic operable to identify said computer file as potentially being a specific known malware free computer file; determining logic operable to determine one or more attributes of said computer file; and comparing logic operable to compare said one or more attributes determined from

said computer file with corresponding stored attributes of said specific known malware free computer file; wherein if said attributes match, then confirming said computer file as being said specific known malware free computer file; and if said attributes do not match then performing further malware detection processing upon said computer file (col. 9, line 10 through col. 10, line 27; col. 12, lines 43-64; col. 13, lines 49-57; col. 14, lines 44-59; and col. 15, lines 17-26).

Conclusion

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-3:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

CR
CR
January 7, 2007

CR
CHRISTOPHER REVAR
PRIMARY EXAMINER